भारतीय मानक
Indian Standard

IS 16695 (Part 1) : 2022

स्कोस्टा : स्मार्ट कार्ड ऑपरेटिंग सिस्टम टेम्पलेट आर्किटेक्चर

भाग 1 बेसिक कमांड सेट

(पहला पुनरीक्षण)

SCOSTA : Smart Card Operating System Template Architecture

Part 1 Basic Command Set

(First Revision)

ICS 35.240.15

© BIS 2022

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

January 2022 **Price Group 10**

FOREWORD

This Indian Standard (Part 1) may be adopted by Bureau of Indian Standards, after the draft finalized by the Identification and Data capture techniques, Cards and Security Devices Sectional Committee, had been approved by the Electronics and Information Technology Division Council.

This standard was originally published in 2018 and is being revised now in order to provide support for the following algorithms in the standard:

a) AES-128, AES-192 and AES-256 based cryptographic operation.

b) SHA-256 algorithm to compute hash.

c) HMAC (Hash-based Message Authentication Code) with SHA1 algorithm to compute hash.

d) HMAC with SHA-256 algorithm to compute hash.

The SCOSTA specification was initially prepared and presented by Indian Institute of Technology, Kanpur, National Informatics Centre and C-DAC, Ministry of Communication and Information Technology, Government of India.

This project was initiated with the following objectives:

a) Standardization of card layout, data fields and other relevant information stored in the card,

b) To ensure interoperability and multivendor support, and

c) To ensure security and integrity of data.

In general SCOSTA compliant operating system based Integrated Circuit Card (ICC) will work with an Interface Device (IFD) using one or more of the protocols, namely ISO/IEC 7816-3 T=0 or T=1; ISO/IEC 14443-3/-4 type A, or type B. Certain examples included here are for illustrative purposes only for better understanding and do not suggest any particular implementation.

This standard describes the minimum support for the application using the ICC. Operating systems with extra features not listed here will be SCOSTA compliant only if they support all the features listed in this standard and the extra features are non-conflicting with the functionality as provided in this standard.

The standard was developed under the sub-committee, LITD 16 : 1 ‘Cards and personal Identification’. The composition of the sub-committee, LITD 16 : 1 responsible for the formulation of this standard is given at Annex B.

CONTENTS

			Page No
1	SCOPE	...	1
2	REFERENCES	...	1
3	SYMBOLS AND TERMINOLOGY	...	1
4	APPLICATION PROTOCOL DATA UNIT (APDU)	...	2
5	TRANSPORT PROTOCOL DATA UNIT (TPDU)	...	3
6	BASIC DATA STRUCTURES	...	3
	6.1 Elementary Files	...	3
	6.2 File Referencing Methods	...	3
	6.3 Data Referencing Methods	...	4
	6.4 File Control Information	...	4
7	SECURITY ARCHITECTURE	...	4
	7.1 Security Status	...	5
	7.2 Security Attributes	...	5
	7.3 Security Environments	...	5
	7.4 Security Algorithms	...	6
	7.5 Security Mechanisms	...	6
	7.6 Access Rule References	...	6
8	APDU MESSAGE STRUCTURE	...	7
	8.1 Coding Conventions for Command Headers	...	7
9	PASSWORD AND KEY REPOSITORIES	...	8
	9.1 Password Repository	...	8
	9.2 Key Repository	...	9
10	COMMANDS	...	10
	10.1 File Related Commands	...	10
	10.2 Security Related Commands	...	12
	10.3 Other Commands	...	16
11	DATA OBJECTS	...	16
12	SECURE MESSAGING (SM)	...	17
13	SESSION KEY DERIVATION	...	18
	13.1 Authentication along with Session Key Derivation	...	18
	13.2 Session Key Derivation using Manage Security Environment Command	...	18
	13.3 Key Derivation for Authentication	...	18
14	SETTING INITIAL VALUE (IV) FOR CRYPTOGRAPHIC METHODS	...	19

Page No

15 CRYPTOGRAPHIC ALGORITHMS ... 19
15.1 Algorithms for Confidentiality ... 19
15.2 Algorithms for Integrity ... 20
15.3 Algorithms for Authentication ... 21
15.4 Algorithm for Hash ... 21
ANNEX A REFERENCES ... 23
A-1 LIST OF REFERRED INDIAN STANDARDS ... 23
A-2 LIST OF REFERRED INTERNATIONAL STANDARDS / PUBLICATIONS ... 23
ANNEX B COMMITTEE COMPOSITION ... 24

LIST OF FIGURES

Fig. 1 Basic Encryption and Decryption Mechanisms in 3 DES Algorithm ... 19
Fig. 2 3 Des Encryption of Large Messages Using CBC Mode ... 20
Fig. 3 ISO/IEC 9797-1 MAC Algorithm 2 Using DES ... 21
Fig. 4 Authentication and Key Establishment Protocol ... 22

LIST OF TABLES

Table 1 Security Algorithms ... 6
Table 2 Coding for the Class Byte in OS ... 7
Table 3 File Control Parameters for Files in the OS ... 11
Table 4 P2 Byte for the VERIFY Command ... 12
Table 5 P2 Byte for Various AUTHENTICATE Commands ... 13
Table 6 Interpretations of P1 and P2 for Various AUTH Commands ... 13
Table 7 Interpretation of Various CRDOs in CRTs for an OS ... 15
Table 8 Interpretation of P1, P2 for PSO Commands ... 16
Table 9 SM Fields for Secure Messaging ... 17

Indian Standard

SCOSTA : SMART CARD OPERATING SYSTEM TEMPLATE ARCHITECTURE

PART 1 BASIC COMMAND SET

(First Revision)

1 SCOPE

This standard (Part 1) specifies the requirement of an operating System that may be put into an integrated circuit that provides a contact, or a contact-less, or a combination of the two interfaces. Such an integrated circuit may be embedded in applications that use contact-less operations such as in an e-passport or may be deployed in a contact-less ID application. It may also be used in a contact interface based applications. This standard also provides details on the Operating System that shall be inter-operable and provide interface for the personalization and initialization.

The following are out of the scope of this standard:

a) The implementation of the operating system,

b) Processor for the smart card and other such details, and

c) The physical communication interface details between the ICC and IFD.

2 REFERENCES

The standards listed in Annex A and Annex B contains provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All Standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated in Annex A and Annex B.

3 SYMBOLS AND TERMINOLOGY

For the purpose of this standard the terms and definitions given in IS 14202 series of standards shall apply, in addition to the following:

'..'	A number in hexadecimal representation (for example, '30' is same as 48)
AM	Access mode byte
AM_DO	Access Mode Data Object
APDU	Application Protocol Data Unit
AT	Authentication template
AT (AUTH)	AT template with usage byte to indicate internal and/or external authentication
AT (USER)	AT template with usage byte to indicate user-knowledge based authentication
CC	Cryptographic Checksum
CCT	Cryptographic Checksum Template
CLA	Class byte for the APDU
CT	Confidentiality template
DATA	Data for the command APDU
DF	Dedicated file
DST	Digital signature template
EF	Elementary file
EFiEF	with SFID of i. 30 ≥ i1
FCP	File control parameters
HT	Hash template
ICC	Integrated Circuit Card (aka smart card)
ID	Identity/Identifier
IFD	Interface Device (aka smart card reader).
INS	Instruction code for the APDU
KAT	Key agreement template
KD	Key for Derivation use
Lc	Coding for Length of DATA in APDU
Le	Coding for Maximum length of RESPONSE expected in APDU
MAC	Message Authentication code

'..'	A number in hexadecimal representation (for example, '30' is same as 48)
Message Digest	A one-way function to calculate MIC from a message
MF	Master File
MIC	Message integrity code (aka MAC)
OS	Operating system
P1	First parameter byte for the APDU
P2	Second parameter byte for the APDU
PCD	Proximity Coupling Device used for interactions with contact-less ICC.
RESPONSE	Response data from the ICC for command APDU
RFU	Reserve for Future Use
SC	Security condition
SCOSTA Compliant OS	Operating System Compliant to this part of the standard
SC_DO	Security condition data object
SE	Security environment
SFID	Short file ID
SHA1	Message Digest Algorithm (Secure Hash Algorithm variant 1)
SM	Secure messaging
SW1	First byte of the status word in the response ADPU
SW2	Second byte of the status word in the response APDU
tAPDU	Transport layer APDU.
tCLA	Class byte for the tAPDU
tDATA	Data for the command tAPDU
tINS	Instruction code for the tAPDU
tLc	Coding for Length of tDATA in tAPDU
tLe	Coding for Maximum length of tRESPONSE expected in tAPDU
tP1	First parameter byte for the tAPDU
tP2	Second parameter byte for the tAPDU
TPDU	Transport Protocol Data Unit.
tRESPONSE	Response data from the ICC for command tAPDU
tSW1	First byte of the status word in the response tADPU
tSW2	Second byte of the status word in the response tAPDU

SECTION I: OPERATING SYSTEM INTERFACE

4 APPLICATION PROTOCOL DATA UNIT (APDU)

For the purpose of this standard, the following two kinds of APDUs are defined. APDU for interface to the transport layer (T=0, T=1, or contact-less type A or type B as defined in IS 14202 (Part 3), ISO/IEC 14443-3 and ISO/IEC 14443-4) is called transport APDU or tAPDU in this standard. The application level APDU shall represent the interface between the application and the OS tAPDU shall have a command header, an optional data field and an option expected length parameter. The command tAPDU shall contain the following:

a) tCLA: CLA byte for the transport APDU;
b) tINS: INS byte in the transport APDU;
c) tP1: P1 byte in the transport APDU;
d) tP2: P2 byte in the transport APDU;
e) tLc: Lc byte related to the transport APDU will be present only when the tAPDU needs command bytes;
f) tDATA: Transport layer data bytes (of size 1.tLc); and
g) tLe: Field in the transport APDU to indicate number of bytes expected in the response tAPDU (transport layer response APDU).

Related fields in the application level command APDU are CLA, INS, P1, P2, Lc, DATA (1..Lc) and Le.

The response tAPDU in the transport layer shall contain the following fields:

a) tRESPONSE: Transport layer response (of size 1..tLe or less); and
b) tSW1, tSW2: transport layer status bytes.

Related fields in the application level response APDU are the following:

a) RESPONSE (1..Le or less). RESPONSE may be absent in the response APDU.
b) b) SW1, SW2.

tAPDU and APDU will have relationship based on certain parameters. If the Secure Messaging is not used, the tAPDU shall be identical to the APDU. If the secure messaging is used, tAPDU shall encapsulate the confidentiality and integrity of the application APDU as is indicated by tCLA.

From the application view point, the maximum size of the Lc and tLc will never exceed 255. The maximum size of the Le and tLe will never exceed 256. All such fields shall be coded in one byte only. The ICC therefore must support short-field Lc and Le and optionally may support extended-field Lc and Le.

5 TRANSPORT PROTOCOL DATA UNIT (TPDU)

Transport Protocol Data Unit (TPDU) shall be used to carry the tAPDU from the IFD to the ICC for command and from ICC to the IFD for the response. Conversion from tAPDU to the APDU shall be carried out completely by the ICC (for the commands) and IFD (for the response) locally. The conversion from APDU to the TPDU shall be based on the transport protocol. For T=0 and T=1 protocols, such conversions are defined in the IS 14202 (Part 3) and for contact-less protocols, such conversions are defined in the ISO/IEC 14443-3, ISO/IEC 14443-4 and IS 14202 (Part 3).

6 BASIC DATA STRUCTURES

The OS shall support the following two categories of the files:

a) Dedicated Files (DF), and

b) Elementary Files (EF).

The file system shall have a tree structure with minimum 4 nodes, so that it will be possible to have one MF, at least one DF under the MF, at least one DF under this DF and one or more EFs under the last DF. At each node of the tree, there can be several children nodes, either of type DF, or of type EF. The root of the tree shall be the Master File (of type DF). At any node of type DF it should be possible to create any number of children nodes (both DF and EF put together). The restrictions on the tree structure, if any will be only because of the limited size of the storage. Under this condition, a CREATE FILE command may fail with an error.

The size of the files will be static and will depend upon the values provided implicitly or explicitly through the File Control Parameters (FCP) declared at the time of CREATE FILE command.

Initially there will be no MF in a fresh, never-powered ICC compliant to this part. At this time, the ICC shall execute no commands except the following:

a) CLA= ‘00’,

b) INS = ‘E0’,

c) P1 = ‘00’, and

d) P2 = ‘00’.

Data field for the command shall indicate the FCP related to the MF.

All commands except CREATE FILE (MF) shall return identical error conditions and fail to execute till the MF is created. MF once created, cannot be deleted.

The ICC shall support data layout for multiple applications each of which may be identified by a DF. The files under the MF will be global for all applications. The files specific to an application shall be stored under a DF node in the file system tree. An application may have sub-applications each represented by an individual DF under the parent DF. In such a case, the application may organize the files as global within the application and local for each sub-application.

6.1 Elementary Files

The elementary files (EF) will be used to keep the data pertaining to an application. An EF can be one of the following types as defined in IS 14202 (Part 4):

a) Transparent EF,

b) Linear EF with fixed size records,

c) Linear EF with variable size records, and

d) Cyclic EF with fixed size records.

The OS may use some EFs internally as well. A few pre-determined and fixed short EF identifiers may be used to identify such EFs. There is however no restriction on the 16-bit identifiers for the same. In particular the OS uses short EF identifiers 1 and 2 internally. Clause 9 of this standard describes their use. A file whose contents may be used by the OS internally shall be declared as INTERNAL EF.

6.2 File Referencing Methods

Each file (an EF or a DF) will have one 16-bit file identifier. The following restrictions shall apply on the 16-bit file identifiers.

a) ‘0000’ and ‘FFFF’ shall be reserved and shall not be used as identifiers;

b) ‘3F00’ will be reserved for the MF and shall not be used for any other file;

c) ‘3FFF’ will be reserved to indicate the current DF and shall not be used for any file;

d) ‘2F00’ and ‘2F01’ shall not be used for any general file under the MF where they are reserved for specific use as defined in IS 14202 (Part 4); and

e) 16-bit File Identifiers will be unique among the identifier for EFs and DFs under a single DF.

The EFs can also be referenced using another short EF identifier (5-bits) given at the time of CREATE FILE command. The following restrictions will apply on 5-bit short file identifiers.

a) Short EF identifiers shall be used only for the files under the currently selected DF.

b) Short EF identifier of ‘00’ and ‘1F’ will be reserved and will not be used for any EF. In particular, short EF identifier of 0, when used, will refer to the currently selected EF. Short EF identifier of ‘1E’ under the MF will also be a reserved one as per IS 14202 (Part 4) and shall not be used for any other general file by the applications.

c) Short EF identifier may not be unique among the EFs under a DF.

d) Short EF identifiers will not be assigned to a file when tag '88' with length 0 is used in the FCP for the file during CREATE FILE command.

e) Short EF identifier will be assigned to the file when tag '88' with length 1 is used in the FCP and the value field indicates a number between 1 and 30. If the value field is a number other than between 1 and 30 (both inclusive), an error shall be returned by the CREATE FILE command.

f) Short EF identifier will be assigned to an EF, when tag '88' is not used in the FCP, as a value given in the least significant five bits of the 16-bit file identifier provided it falls between 1 and 30 (both inclusive). In case, this value is 0 or 31, the short EF identifier shall not be assigned.

g) While selecting a file using short EF identifier, the results will be unpredictable if two or more files exist with the same short EF identifier.

h) Under any DF, there can be a maximum of one EF which is of type internal and has an SFID='01'. Same restrictions will also apply for an internal EF with SFID='02'.

Each DF in the file system may also have a DF name that shall be unique among all DFs in the file system. This DF name can be specified in the FCP during the CREATE FILE command. It will be possible to refer to a DF with its name irrespective to its location in the file system when the name was specified during the CREATE FILE command. When the DF name is not specified, it will not be possible to refer to that DF by its name.

Files can be referenced using the following four methods as described in IS 14202 (Part 4).

a) Referencing by the file identifier. The values '3F00', '3FFF' and 'FFFF' are used for special purposes as given in IS 14202 (Part 4) standard. In addition to this, the file IDs '2F00' and '2F01' under the MF shall also be reserved.

b) Referencing by path. The path starting with '3F00' shall refer to the absolute paths (that is starting from the MF) while the paths starting from any other file identifier will refer to the relative paths (that is starting from the current DF). Paths starting from '3FFF' will also refer to the paths starting from the current DF. '3F00' and '3FFF' can occur only in the beginning of a path. For example, a path such as '3F003F00' shall be considered as a wrong path.

c) Referencing by short EF identifier. Valid SFID will be a value in the range 1 to 30 (that is '01' to '1E') and will be coded appropriately in the commands. An SFID of 0 will refer to the currently selected EF. There may be multiple files with the same SFID.

d) Referencing by DF name. DF name referencing will be possible only for the DFs which were created with the name given in the FCP. The file name shall be unique among all DFs in the ICC. In case, two DFs are given the same name, the behaviour of the SCOSTA compliant OS is not specified.

6.3 Data Referencing Methods

The OS shall implement at least the following data referencing methods as defined in IS 14202 (Part 4).

a) Record referencing:

1) Referencing by one byte record number; and

2) Referencing by one byte record identifier.

It is implied in this standard that the maximum size of a record shall not exceed 255 bytes.

b) Data Unit referencing

The data unit referencing shall be available for the transparent EF. The operating system may implement data unit referencing mechanism for the record structure files as well primarily intended to debug the applications. However, in such a case, the data returned may include the structural information (meta-data) as well. An application to interface with an OS shall make no assumptions about the structure of the meta-data.

The ICC may support variable data unit size (among these support for 8-bits wide data units is mandatory for all OS) as defined in IS 14202 (Part 4).

6.4 File Control Information

File control parameters shall be supported for CREATE FILE command as well as for SELECT FILE command.

The OS shall support the FCP templates to be returned to the application during the SELECT FILE command execution. In case SELECT FILE command demands other templates, meaningful default information should be supplied if the other templates are not supported.

7 SECURITY ARCHITECTURE

In the OS, resources may be protected against various operations. These resources include files, DOs and commands. While checking for the security applicability, first the command level security shall be applied and only if successful, the individual resource level security will be applicable. For example, if a file is permitted to have a read access but the execution of READ BINARY command is subjected to certain security condition, the file can only be read if the READ BINARY security condition is met. This part supports the secure messaging and therefore it will be possible for a resource to be utilized only under SM commands if such an access condition is specified.

The OS shall support the security architecture as defined in IS 14202 (Part 4), IS 14202 (Part 8) and IS 14202 (Part 9).

7.1 Security Status

The OS shall support the following three kinds of security status.

a) Global security status (related to the MF authentication processes),

b) File-specific security status (related to the DF authentication processes), and

c) Command specific security status (related to the command authentication processes which are specific to the currently selected DF).

7.2 Security Attributes

It shall be possible to attach security attributes to the files using the FCP [as given in IS 14202 (Part 4)]. Both compact and expanded forms of security attributes must be supported.

The OS shall support the access mode bytes (AM bytes) as defined in IS 14202 (Part 4) for EF and DF. Other kinds of AM bytes (for example AM bytes for DOs and tables etc.) are optional for the OS. No proprietary coding shall be used in AM/SC bytes.

There may be several SC bytes for each AM byte when the security attributes are specified in the compact form (tag '8C' in the FCP). The number of SC bytes depends upon the number of bits set to 1 in the corresponding AM byte. Under tag '8C' there may be several groups of AM and associated SC bytes. In case, an operation is covered by more than one such group, an OR condition shall prevail, that is any of the conditions may be satisfied. In a similar manner, when the security attributes are specified using expanded form (tag 'AB'), there may be several groups of AM_DO and SC_DOs. In such cases when an operation is covered by several of these groups, an OR condition shall prevail.

In a group if the AM_DO provides an AM byte, the number of SC_DOs shall be equal to the number of bits set to 1 in the AM byte. In all other cases, an AND condition shall prevail if multiple SC_DOs are specified.

Security attributes of the command can only be specified using the expanded form. Security attributes of the file operations can be specified using the compact form and when it refers to a particular SE, the SE shall be looked for the CT and CCT tag(s) for the SM related security and AT tag(s) for the authentication (entity or user authentication). The usage qualifier bytes shall be consulted for the considered CRT.

Security attributes of command shall be applicable based on the currently selected DF only. That is only the security attributes for the currently selected DF shall be applicable for the access control related to the commands.

If a DF or EF is in the terminated state, the only operations possible on it are selection and deletion. If a DF or EF is in the deactivated state, the only operations possible on it are selection, activation, termination, and deletion. Further, no commands are permitted if a DF in the terminated or deactivated state is the current DF. Any command that specifies a file (EF or DF) by path shall fail if a terminated or deactivated DF is one of the components but not the final component in the path.

7.3 Security Environments

The security environments (SEs) shall be stored either in an EF or in the FCP of the DF with a tag '7B'. In case the SEs are stored in an EF, the 16-bit file id of the EF shall be notified with tag '8D' in the FCP of the corresponding DF. Such an EF can only be under the DF for which the SEs are being defined. When a DF is selected, the SE#1 for that DF will be selected as current SE automatically. In case, there is no definition of the SE#1, the current SE in force will be all empty. When the DF is created first and the corresponding SE file is not yet created, the current SE will be all empty (since the created DF becomes the current DF). Upon selection of such a DF, the current SE will also be all empty. The current SE will not be modified when the SE file is created and written into. It shall only be modified when the DF is selected again.

The SEs are also selected using MANAGE SECURITY ENVIRONMENT (MSE) command. When a DF is selected or when the current SE is changed using MSE: RESTORE command, the definition of the previously selected SE will not be in force. In this case, the IV, IV update mode, derived keys, challenge, etc. shall be derived from the values provided in the new SE definition, or reverted to the default in case they are unspecified in the new SE definition. OS shall support at least the following CRTs in the definition of the SEs.

a) *Confidentiality Template (CT)* — CT shall be identified by tag 'B8'. CT will be subjected to the usage qualifier byte. If the usage qualifier byte is not specified the CT template will be applicable for all operations under all conditions.

b) *Cryptographic Checksum Template (CCT)* — CCT shall be identified by tag 'B4'. CCT shall be subjected to the usage qualifier byte. If the usage qualifier byte isnot specified, the CCT template shall be applicable for all CC operations under all conditions.

c) *Authentication Template (AT)* — AT shall be identified by tag 'A4'. AT can be defined for the cryptographic authentication and/or user knowledge (PIN/Password) based authentication based on the usage qualifier. If the usage qualifier is not specified the AT template shall be applicable for all authentication related operations under all conditions.

d) *Hash Template (HT)* — HT shall be identified by tag 'AA'.

OS may support additional optional CRTs (for example, DST etc.)

7.4 Security Algorithms

The OS shall support algorithms given in Table 1 for message digest, confidentiality, integrity and authentication. Details about these algorithms are given in 15.

7.5 Security Mechanisms

The OS shall support the following security mechanisms [*see* IS 14202 (Part 4)].

a) Entity authentication with password (VERIFY command);

b) Entity authentication with key (EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE and MUTUAL AUTHENTICATE commands). These mechanisms will be subjected to the algorithms as defined in 7.7 and may also include the facility to be able to establish a session key;

c) Data authentication (computation/verification of cryptographic checksum). These mechanisms will be subjected to the algorithms as defined in **7.4**;

d) Data encipherment and decipherment. These mechanisms shall be subjected to the algorithms as defined in 7.4.

e) Computation of message digest (Hash) code for the data. The mechanism for the computation of hash shall be subjected to the algorithms as defined in **7.4**.

f) Secure messaging with confidentiality and Integrity requirements. Secure messaging for the OS is explained later in this document. These mechanisms shall be subjected to confidentiality and integrity algorithms as defined in **7.4**.

7.6 Access Rule References

The access rule (in expanded or in compact format) for a file can be stored in the file's FCP. These rules shall specify under what security conditions certain operations on that file are permitted. The access rules for the DOs can be stored in the FCI of the corresponding DF. The access rule referencing mechanisms shall be according to IS 14202 (Part 4).

Table 1 Security Algorithms

(*Clauses* 7.4 *and* 9.2)

Algorithm Reference Byte Value	CRT Template to which Applicable	Algorithm
00 (Default) and 01	CT	3DES (Enc and Dec)
82	CT	AES-128 (Enc and Dec)
83	CT	AES-192 (Enc and Dec)
84	CT	AES-256 (Enc and Dec)
01	CCT	3DES based CBC Residue (CC Computation and Verification) ISO/IEC 9797-1 Algorithm 1 for MAC using TDES
00 (Default) and 02	CCT	ISO/IEC 9797-1 Algorithm 2 for MAC using DES
83	CCT	AES-128 based CBC Residue (CC Computation and Verification) with ISO/IEC 9797-1 Algorithm 1 for MAC using AES-128.
84	CCT	AES-192 based CBC Residue (CC Computation and Verification) with ISO/IEC 9797-1 Algorithm 1 for MAC using AES-192.
85	CCT	AES-256 based CBC Residue (CC Computation and Verification) with ISO/IEC 9797-1 Algorithm 1 for MAC using AES-256.
00 (Default) and 01	AT (AUTH)	3DES based challenge response
02	AT (AUTH)	ISO/IEC 11770-2 Key Establishment Mechanism 6 using 3DES
83	AT (AUTH)	AES-128 based challenge response
84	AT (AUTH)	AES-192 based challenge response
85	AT (AUTH)	AES-256 based challenge response
00 (default) and 01	HT	SHA-1 as defined in FIPS-140
02	HT	SHA-256 as defined in FIPS-140
03	HT	HMAC (Hash-based Message Authentication Code) with SHA-1
04	HT	HMAC with SHA-256

Table 2 Coding for the Class Byte in OS

(*Clause* 8.1.1)

Class Byte								Meaning
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	Commands in plain with no secure messaging
0	0	0	0	1	1	0	0	SM with authenticated command header
0	0	0	0	1	0	0	0	SM without authenticated command header
Other								RFU for this part

8 APDU MESSAGE STRUCTURE

The OS shall support at least the normal 1-byte fields for coding Le and Lc (tLe and tLc for tAPDU) fields in the command APDU/command tAPDU [as defined in IS 14202 (Part 4)]. An APDU can be communicated with or without secure messaging. In case of secure messaging the corresponding tAPDU received shall contain one or more security mechanisms applicable to the command and the ICC shall send the response tAPDU with applicable secure messaging as defined by the received command for which the response is generated.

8.1 Coding Conventions for Command Headers

The command header has four bytes (CLA, INS, P1 and P2 for the APDU and tCLA, tINS, tP1 and tP2 for the tAPDU).

8.1.1 *Class Byte (CLA and tCLA)*

The class byte coding as given in Table 2 shall be applicable to the OS.

In particular tCLA will have a value of ‘00’ or ‘08’ or ‘0C’. The CLA will have support only for the ‘00’ value.

8.1.2 *Instruction Byte (INS, tINS)*

Instruction bytes shall be coded as defined in IS 14202 (Part 4), IS 14202 (Part 8) and IS 14202 (Part 9), in the appropriate places. In this part, only even INS bytes are to be used. Provision of odd INS byte codes shall not result in non-compliance to this part. The instructions that shall be implemented as mandatory instructions in an OS are described in this part of the standard.

In case the secure messaging data objects contain the command header (under tag ‘89’), the INS byte shall be taken from that data object and not from tINS. Otherwise the INS byte shall be same as the tINS. In the former case, the command may be protected from the eavesdropper wherein the transport layer instruction byte (tINS) has no resemblance to the command being executed.

8.1.3 *Parameters to the Instructions (P1, P2, tP1 and tP2)*

P1 and P2 bytes shall be coded as described for the individual instructions in IS 14202 (Part 4), IS 14202 (Part 8) and IS 14202 (Part 9). The further interpretation of these bytes and restrictions if any are given in this standard at appropriate places. In case the SM data objects contain the command header (under tag ‘89’), the tP1 and tP2 bytes shall be ignored and the P1 and P2 bytes shall be taken from the command header in the SM data objects. Otherwise the P1 and P2 shall be identical to tP1 and tP2.

8.1.4 *Data Field (DATA, tDATA)*

The data fields of the command APDU and command tAPDU shall be coded as per the transport protocol of ISO/IEC 14443 (Part 4). When there is secure messaging in force, tDATA field shall be a collection of SM data objects which shall be made from one or more of the following fields of the APDU.

a) Command Header (CLA, INS, P1 and P2),
b) DATA,
c) Le, and
d) Cryptographic checksum of one or more fields.

If secure messaging is not used, the tDATA field shall be identical to DATA field.

8.1.5 *Response Data Field (RESPONSE, tRESPONSE)*

The data fields in the response APDU and response tAPDU shall be coded as per the transport protocol of the ISO/IEC 7816 or ISO/IEC14443 standards as the case may be. In case secure messaging is used, the tRESPONSE shall be a collection of SM DOs and will be derived from the following fields of the response APDU.

a) RESPONSE,
b) SW1 and SW2, and
c) Cryptographic checksum of one or more fields.

In case, secure messaging is not used, the tRESPONSE field shall be identical to the RESPONSE field.

8.1.6 *Status Bytes (SW1, SW2, tSW1 and tSW2)*

These bytes are coded as described inIS 14202 (Part 4), IS 14202 (Part 8) and IS 14202 (Part 9) and suitably interpreted in this standard at appropriate places. If secure messaging is used, the tSW1 and tSW2 shall carry only the secure messaging related status (that is '6987': Expected secure messaging DOs missing; and '6988': Incorrect secure messaging DOs). An SM data object in the response of tAPDU will provide the SW1 and SW2 (processing status of the command). If SM is not used, tSW1 and tSW2 shall provide the SW1 and SW2.

9 PASSWORD AND KEY REPOSITORIES

In an OS, PIN and passwords are generally stored in identical manner and therefore are indistinguishable. In this standard, terms "password" and "PIN" are used in a generic manner to indicate PIN as well as password and will be used for User-knowledge based authentication. Passwords and keys are stored in elementary files in the OS. The following rules shall apply:

a) The passwords are stored in an elementary file EF1 (file with a short file id of 1) at various levels of directories.

b) A valid password repository will be an INTERNAL record file (variable or fixed size).

c) There can only be one password repository under any DF (There can bemultiple files with short file id of 1 but only one of them can be an internal record file).

d) The global passwords are stored in password repository (EF1) under the MF.

e) When the current directory is MF, global and local passwords will mean the same.

f) There can be up to a maximum of 31 records in any password repository (that is EF1). A password repository can store passwords whose identifiers can have a value between 1 and 31 (both inclusive).

g) The keys are stored in a key repository in an elementary file EF2, a file with a short file id of 2 at various levels of directories.

h) A valid key repository will be a record file (variable or fixed size) and will be an INTERNAL EF.

j) There can only be one key repository under a DF. There can be multiple files with short file id of 2 but only one of them can be an internal record file.

k) The global keys are stored in EF2 under MF. When the current DF is the MF, the local and global keys will be the same.

m) There can be a maximum of 31 keys in a key repository with key identifiers carrying unique values from 1 to 31 (both inclusive).

n) The OS and/or applications may choose any 16-bit file ids for password and key repositories.

As passwords are verified, the OS shall maintain the status of those passwords (verified/not-verified) at each level from the MF to the currently selected DF. Similarly as keys are authenticated, the OS shall maintain the status of those keys (authenticated/non authenticated) at each level from the MF to the currently selected DF. The statuses of the keys and passwords for a DF are maintained when currently selected DF is modified (possibly due to the SELECT FILE or any other command) if the DF lies in the common part of the paths from the MF to the old DF and from the MF to the new DF. The status of keys and passwords for all other DFs are treated as "not-verified" and "non-authenticated".

A password corresponding to password reference specified in the password related commands such as a VERIFY command, or in an SE under the AT template with User-knowledge based key reference, may not be found. Similarly, a key reference specified in a key based command such as in INTERNAL/EXTERNAL/ MUTUAL AUTHENTICATE command, or in an SE under any of the CRT that refers to the cryptographic keys may not be found. This condition may happen due to one of the following reasons:

a) The corresponding password or key repository does not exist; and

b) The repository exists but no record is found corresponding to the referred key or password.

In such a case, the corresponding commands shall return a failure condition ('6A88', for "reference data not found") whenever applicable.

The changes in the password/key may or may not be permitted depending upon the security attributes for that file.

9.1 Password Repository

The password repository shall be a variable/fixed record file (up to a maximum of 31 records) with the following data items (in the same order):

a)	Pin identifier	1 Byte
b)	Retry counter	4 Bits (see below)
c)	Max retry count	4 Bits (see below)
d)	Pin	Variable length

The pin identifier shall be coded as follows.

b8	b7	b6	b5	b4	b3	b2	b1
V	RFU		Ref Data Number				

V bit represents if the corresponding entry is valid (1) or not (0). The password related commands such as VERIFY command for the invalid data will return

a failure ('6984', "Reference data not usable") in the status bytes. For the purpose of security attributes of a file operation, an invalid password or a non-existent password is considered as "VERIFIED".

V bit is manipulated using the ENABLE VERIFICATION REQUIREMENT and DISABLE VERIFICATION REQUIREMENT commands.

Records in the EF1 will have one byte containing the Retry counter and Max retry count. The bits b_8: b_5 of this byte will provide the Retry counter while bits b_4:b_1 will provide the Max retry count. Bits b_8 and b_4 will be the MSB of their respective fields. A value 'F' for the Max retry count with non-zero retry counter mean that there is no limit on the retries.

If Max retry count is a value other than 'F', then upon a successful verification, retry counter for that reference data is set to the Max retry count. Also upon unsuccessful verification, Retry counter decrements by 1 and when it reaches a value of 0, subsequent VERIFY commands return a failure without any verification.

If Max retry count is 'F' (but the Retry counter is non zero) then no limit will be set on the number of retries. In such a case, the Retry counter shall not be changed after a successful or unsuccessful verification.

If the Retry counter is zero, then VERIFY command returns a failure without any verification irrespective of the value of the Max Retry Count.

9.2 Key Repository

The key repository is an internal EF containing variable/ fixed records (up to a maximum of 31 records) with the following data items (in the same order) in each record:

a)	Key identifier	1 Byte
b)	Key Type	1 Byte
c)	Key Specific Information	Variable length
d)	RFU Byte	1 Byte
e)	Key	Variable length

The key identifier shall be coded as follows.

b8	b7	b6	b5	b4	b3	b2	b1
V	RFU		Key Number				

V bit is used to denote if the corresponding key is valid or not. (0: invalid; 1: valid). The key number (by which the key is referred to in various security related operations) shall be unique for all keys. There can be only up to 31 keys in EF2. No two keys shall have the same key number even if they are used for two different purposes.

The key type field provides the operations for which the key can be used. The value is coded as follows.

b8	b7	b6	b5	b4	b3	b2	b1
CC	RFU	Enc	RFU	RFU	RFU	Int Auth	Ext Auth

If the CC bit is set to 1, the key can be used for computation and verification of the cryptographic checksum.

If the Enc bit is set to 1, the key can be used for symmetric encryption and decryption.

If the KD bit is set to 1, the key will be known as a master key and can only be used for derivation. A master key is not intended for direct use. In the case of a master key record, all other bits and information refer to the derived key and not for the master key.

If the Int Auth bit is set to 1, the key can be used for the internal authentication.

If the Ext Auth bit is set to 1, the key can beused for the external authentication.

If the key is to be used for the Mutual Auth, bit b_1 and b_2 both should be set to 1 in the key type field. The type specific information is of variable length and is defined as per the key type field. The value is made available for each bit set to 1 in the key type field. The values are provided in the order of the bits in the key type field. Thus if the CC bit is set to 1, the type specific information will first contain the information regarding the usage of the key for the CC. The following type specification information is used.

Operation	Information
CC	None (0 bytes)
Enc	Usage Counter (2 Bytes)
KD	None (0 bytes)
Int Auth	Usage Counter (2 Bytes)
Ext Auth	Retry Counter (4 bits) and Max Retry Count (4 bits)

The following rules shall apply for the usage counters:

a) Usage counters for the Enc, and Int Auth are monotonically decreasing counters.

b) The counter if set to 'FFFF', means that the counter is not used (and therefore is not changed by the usage of the key – count treated as infinity).

c) Values other than 'FFFF' refer to the number of times that the key can be used by the respective operations.

d) The Int Auth counter will be decremented each time INTERNAL AUTHENTICATE command is used unless it is '0000' or 'FFFF'.

e) The Enc counter is decremented each time a PSO:ENCRYPT or PSO: DECRYPT, SM:ENCRYPT or SM:DECRYPT operation is performed using this key as long as it is not '0000' or 'FFFF'.

f) The key can be used only if the Usage Counter is non-zero.

g) The initial value of the counter is set at the time of writing the record in the EF2. The value can be changed by UPDATE RECORD command if its execution is permitted by the security conditions.

The retry counter and max retry count are coded as per the coding given for the password repository. Bits b8:b5 provide the Retry Counter value while bits b4:b1 provide the max retry count. These values are used only upon the use of the EXTERNAL AUTHENTICATE/ MUTUAL AUTHENTICATE commands. If the value of the retry counter is 0, the relevant command results in a failure. If the retry counter is other than 0, it is decremented by 1 (only if the max retry count is not 'F') upon each unsuccessful authentication. Retry counter is set to max retry count after each successful authentication.

The RFU byte in the key record will always be '00'.

The changes in the EF2 may or may not be permitted depending upon the security attributes for that file. However, this file will be referenced for validating the keys internally by the operating system.

An invalid key will result in a failure for all commands that may use this key. However for the security conditions, an invalid key is assumed to have been satisfied. For example, if a file read operation is subject to the condition of proving the knowledge of a key which is marked invalid, the read operation shall be permitted.

The appropriate algorithm will be chosen for the operation as given in Table 1. If the key is not permitted to be used for the operation (as per the key-type information), SW1-SW2='6985' ("Condition of use not satisfied") will be returned.

10 COMMANDS

An ICC has two kinds of storage, volatile and non-volatile. All instructions that update the non-volatile storage shall execute automatically. The effect of all such commands will be either due to the complete execution or due to no execution. The ICC may use the subsequent power up to finish the last command. The commands described in this part are categorized as follows:

a) File related commands,

b) Security related commands, and

c) Other commands.

All of these commands are appropriately referred in various parts of IS 14202.

10.1 File Related Commands

The OS shall support the commands given in below as per the standard given in the last column.

	Command	Reference Standard
a)	READ BINARY command	IS 14202for INS = 'B0'.
b)	READ RECORDS command	IS 14202 for INS = 'B2'.
c)	WRITE BINARY command	IS 14202 for INS = 'D0'.
d)	WRITE RECORD command	IS 14202 for INS = 'D2'.
e)	UPDATE BINARY command	IS 14202 for INS = 'D6' (Also see ERASE BINARY command for some details on UPDATE BINARY.)
f)	UPDATE RECORD command	IS 14202 for INS = 'DC'.
g)	APPEND RECORD command	IS 14202 for INS = 'E2'.
h)	ERASE BINARY command	IS 14202 for INS = '0E'.

An EF is either created with the CREATE FILE command or is available in the ICC initially. The maximum size of the EF is fixed in the beginning. The EF will have the initial state of data as 'invalid'. Data added in the EF makes its state as 'valid'. ERASE BINARY command is used to delete the contents previously added using WRITE BINARY command. Such a command for the EF with a record structure is not needed as the record structures themselves may have a status byte (valid/invalid) and the applications can manipulate them by UPDATE RECORD command.

Depending upon the attributes of the file, ERASE BINARY command will initialize the file data to all 1's (for write-and files) or to all 0's (for write-or files). For write-once files, the flags shall be maintained at the level of each data-unit and it will be possible to erase data in units of one data-unit. Upon ERASE BINARY, the flags will be set to appropriate values.

The UPDATE commands will only modify the data and disregard the flags. Thus it will be possible to UPDATE data and later WRITE into a write-once file, if the file has not been written into.

For maintaining the atomicity, the OS may assume that an application shall not issue an erasure of more than 255 bytes at a time. In case, the application issues an erasure of more than 255 bytes, the command shall still be carried out even though atomicity for the command may not be guaranteed.

10.1.9 *CREATE FILE Command*

Ref: As in IS 14202 for INS = 'E0'.

The CREATE FILE command in the OS will require the file control parameters as given in Table 3.

The OS shall support P1 and P2 bytes of the command to be all 0s. Implementation with other values of the P1

and P2 is not mandatory in an SCOSTA compliant OS. If such cases are implemented, a default value of the FCP may be assumed.

The default value for the LCSI of a file created using CREATE FILE command (if not explicitly specified in the command) will be '05' (operational state-activated).

At most one PIN repository (internal EF with SFID of '01') can be created within a DF. Similarly, at most one key repository (internal EF with SFID of '02') can be created within a DF. If an attempt is made to create a PIN repository (or a key repository) in a DF that already contains one PIN repository (or one key repository), the command should return an error.

10.1.10 *DELETE FILE Command*

Ref: As in IS 14202 for even INS = 'E4'.

a) The DELETE FILE command can be used to delete an application/sub-application in a multi-application ICC or delete an EF within a single application. For deleting a file, the following two security conditions are applicable;

b) "DELETE FILE (child)" of the parent DF of the EF/DF to be deleted; and

c) "DELETE FILE (self)" of the EF/DF to be deleted.

If the DELETE FILE command is used to delete a DF, the entire sub-tree under that DF is deleted. However, this command cannot be used to delete the MF. After successful execution of this command, the parent DF of the deleted EF/DF becomes the current DF. If as a result of the execution of the command, the current DF changes, then after the execution of the command, the current EF of the card is undefined; otherwise, it remains the same as before. If the current DF is changed, the current SE and related data are also changed.

Table 3 File Control Parameters for Files in the OS

(*Clause* 10.1.9)

Tag	Value	Applicable to
'80'	Size of the file in bytes	Transparent EF
'82'	Depending upon the length	
(L=1)	File descriptor byte-FDB (Mandatory field	All files
(L=2)	FDB + data coding byte-DCB	Transparent EF
(L=5)	FDB + DCB + MRL (2 bytes	EF of records
(L=6)	FDB + DCB + MRL (2 bytes	EF of records
	NOTE — Tag '82' with length 3 and 4 is defined in **IS 14202 (Part 4)** but is not used with these values of the length in this part. Tag '82' with length 1 and 2 is defined in **IS 14202 (Part 4)** for any file. In an SCOSTA compliant OS, these can be used only for the DF and transparent EF respectively.	
'83'	File identifier (Mandatory field	Any file
'84'	DF Name	DFs
'88'	Short EF identifier (1 SFID 30	EFs
	NOTE — If this tag is not present, least five bits of the File identifier (tag '83') be used as short EF identifier (unless they represent 0 or '1F'). If this tag specifies no value (length 0), the corresponding EF will have no short EF identifier. In case, multiple files are found with same SFID, the behavior of the subsequent commands with implicit selection based on SFID is undefined. In case, it results in a conflict with the key or password repository, CREATE FILE command shall fail.	
'8A'	Life Cycle Status Integer (LCSI	Any file
'8C'	Security attributes in compact form	Any file
'AB'	Security attributes in expanded form	Any file
	NOTE — If the security attributes are not defined in expanded or in compact form, default security attributes of 'no security' will be used. Thus the information in a file with no security attribute can be operated upon by an application.	
'7B'	SEs as defined in IS 14202 (*see also* 7.3). SEs may be contained in an EF in which case tag '8D' is to be used to provide the file id.	DFs
'8D'	File id of the EF under the DF containing SE templates. The SEs can be specified using '7B' tag also.	DFs

10.1.11 *SELECT FILE Command*

Ref: As in IS 14202 for INS = ‘A4’.

It should be possible for the SELECT FILE command to return FCP of the selected file depending upon the value in parameter P2. If Le field is empty, no value will be returned by the SELECT FILE command. The ICC must indicate the number of byte available using ‘61XX’ status. These can be retrieved by the IFD with the help of a GET RESPONSE command. When P2 is between ‘0C’ to ‘0F’, no value shall be returned and indication of the number of bytes using ‘61XX’ shall not be given.

When the current DF is changed, the current SE and related data are also changed.

10.1.12 *ACTIVATE FILE Command*

Ref: As in IS 14202 for INS = ‘44’.

Similar to the SELECT FILE command, it will be possible for the application to get the FCP of the file depending upon the value in the parameter P2. The LCSI byte in the returned FCP will represent the status of the file after the execution of the command.

10.1.13 *DEACTIVATE FILE Command*

Ref: As in IS 14202 for INS = ‘04’.

Similar to the SELECT FILE command, it will be possible for the application to get the FCP of the file depending upon the value in the parameter P2. The LCSI byte in the returned FCP will represent the status of the file after the execution of the command. In case of a DF, this command will execute successfully only if all EFs and DFs that exist immediately within the DF to be deactivated are already in the deactivated or terminated state.

10.1.14 *TERMINATE DF Command*

Ref: As in IS 14202 for INS = ‘E6’.

Similar to the SELECT FILE command, it will be possible for the application to get the FCP of the file depending upon the value in the parameter P2. The LCSI byte in the returned FCP will represent the status of the file after the execution of the command. This command will execute successfully only if all EFs and DFs that exist immediately within the DF to be terminated are already in the terminated state.

10.1.15 *TERMINATE EF Command*

Ref: As in IS 14202 for INS = ‘E8’.

Similar to the SELECT FILE command, it will be possible for the application to get the FCP of the file depending upon the value in the parameter P2. The LCSI byte in the returned FCP will represent the status of the file after the execution of the command.

10.1.16 *TERMINATE CARD USAGE Command*

Ref: As in IS 14202 for INS = ‘FE’.

This command is functionally the same as terminating the MF using the TERMINATE DF command and can only be executed if all EFs and DFs that exist immediately within the MF are already in the terminated state.

10.2 Security Related Commands

The OS shall support the commands given in **10.2.1** to **10.2.11**.

10.2.1 *VERIFY Command*

Ref: As in IS 14202 for INS = ‘20’.

VERIFY command in the OS is used to verify the password with the password stored in the ICC. The reference data number as provided in P2 should be interpreted as given in Table 4.

When the value of P2 is 0, the PIN number shall be taken from the AT template of the currently selected SE for which the usage qualifier indicates the user knowledge based authentication. The error conditions shall be returned as if the reference data is not found if any of the following conditions are true:

a) No CRT with AT template is found in the current SE;

b) Key reference (to be interpreted as PIN reference) is not specified in the AT template;

c) Usage qualifier does not permit the user knowledge based authentication; and

d) The PIN is not found in the repository or the corresponding record is an invalid one.

Table 4 P2 Byte for the VERIFY Command

(*Clauses* 10.2.1 *and* 10.2.9)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information is given
0	0	0	X	X	X	X	X	PIN number in the global PIN repository
1	0	0	X	X	X	X	X	PIN# (lower 5 bits) in the local repository
All other values								RFU

Table 5 P2 Byte for Various AUTHENTICATE Commands

(*Clause* 10.2.2)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information is given
0	0	0	X	X	X	X	X	Key Reference in Global Key Repository
1	0	0	X	X	X	X	X	Key Reference in local Key Repository
All other values								RFU

If the most significant bit of the PIN number is 1, then the PIN number coded in the lower five bits shall refer to the PIN in the local repository. If the most significant bit of the PIN number is 0, then the PIN number shall refer to the PIN in the global repository.

10.2.2 *INTERNAL AUTHENTICATE Command*

Ref: As in IS 14202 for INS = '88'.

The description for the INTERNAL AUTHENTICATE command is also valid for the MUTUAL and EXTERNAL AUTHENTICATE commands and is indicated explicitly.

The INTERNAL/EXTERNAL/MUTUAL AUTHENTICATE command requires an algorithm reference in P1 and a key reference in P2 as per Table 5.

Depending upon the values of P1 and P2 for INTERNAL/EXTERNAL/MUTUAL AUTHENTICATE commands, key reference and algorithm references may be taken from the current SE, P1 or P2 as per Table 6. When the references are taken from the current SE, the AT template shall be used for which the usage qualifier permits the selected operation.

Table 6 Interpretations of P1 and P2 for Various AUTH Commands

(*Clause* 10.2.2)

P1	P2	Value of Algo Ref	Value of Key Ref
0	0	From current SE	From current SE
0	≠0	From current SE	P2
≠0	0	P1	From current SE

An error ('6A88': REFERENCE DATA not found) shall be returned when any of the following conditions are true:

a) If there is no CRT with AT template in the current SE;

b) The key reference is not specified in the AT template of the current SE. (When the Algorithm Reference is not specified in the AT template, it shall be taken as 0). See also **10.2.4** for MUTUAL AUTH specific details;

c) The usage qualifier in the SE does not indicate the use for the command;

d) The key is not found in the key repository; and

e) The indicated algorithm is not supported.

The value of AlgoRef as indicated in Table 6 when 2, the INTERNAL and EXTERNAL AUTHENTICATE commands equals will fail and only MUTUAL AUTHENTICATE command shall be allowed to proceed to establish session key along with the authentication.

The INTERNAL/EXTERNAL/MUTUAL AUTHENTICATE commands shall return error when any of the following conditions are true (but for the exceptions as listed below):

a) If the key is found in the repository but is an invalid one. In this case the behaviour for the EXTERNAL AUTH command shall be as indicated in **10.2.3**. Otherwise an error code '6984' (Reference data not usable) shall be returned.

b) The key type byte in the key repository (or for the derived key in case of master key usage) does not permit the command. An error code ('6985': condition of use not valid) shall be returned.

c) If the key is found to be expired (that is, the usage counter is 0). An error code '6985' shall be returned.

The response is not as expected for the challenge (in case of MUTUAL/EXTERNAL AUTHENTICATE).

If the indicated key reference is provided under tag '84' (key for the derived key usage) then the derived key shall be used rather than the master key itself. In this case, the key repository must also indicate the key to be a master key by the KD bit set to 1. The key must have been derived for the appropriate use (for internal authentication in case the command is INTERNAL AUTH; for external authentication in case the command is EXTERNAL AUTH; and for both in case the command is MUTUAL AUTH) using MANAGE SECURITY ENVIRONMENT command.

For the INTERNAL AUTHENTICATE command, corresponding 16-bit usage counter shall be decremented by 1 unless it is 0 or 'FFFF'.

10.2.3 *EXTERNAL AUTHENTICATE Command*

Ref: As in IS 14202 for INS = '82'.

The EXTERNAL AUTHENTICATE command will be subjected to the behavior as described in **10.2.2**. In addition the following shall apply:

a) If the body of the command is empty, SW1-SW2 = '63CX' (where X is the value of further allowed retries) will be returned if the record corresponding to the referenced key is valid. In this case, no counters will be modified.

b) If the body of the command is empty, SW1-SW2 = '9000' will be returned if the record corresponding to the referenced key indicated key to be invalid. No counters shall be modified in this case.

c) If the reference data is invalid and the body is non-empty, '6984' (REF DATA NOT USABLE) shall be returned.

When the authentication is successful (the response is as expected for the issued challenge), retry counter shall be set to the maximum retry count, otherwise the counter shall be decremented by 1.

10.2.4 *MUTUAL AUTHENTICATE Command*

Ref: As in IS 14202 for INS = '82'.

The MUTUAL AUTHENTICATE command will be subjected to the behavior as described in **10.2.2**. In addition the following shall apply:

a) The behavior of this command shall be same as an EXTERNAL AUTH followed by an INTERNAL AUTH. This command may be used for the derivation of session keys as described later in **13.1**. When the MUTUAL AUTH command is used for key derivation and authentication purposes as outlined in section 2.1 of Part II, the command needs to perform operations related to confidentiality as well as integrity. For this purpose, the confidentiality and integrity keys shall be taken from the CT and CCT templates. In such a case, valid values of P2 must only be 0.

b) When the mutual auth is used only for the authentication, the key reference for this command (as given in Table 6) will be valid only if the key type indicates that the key can be used for Internal Authentication as well as for External Authentication.

c) When the mutual auth is used for key derivation as well, the key for confidentiality must be valid for encryption and decryption (in the CT template of the SE) and the key type must permit encryption. The key for the integrity must be valid for computation and verification of crypto-checksum (in the CCT template of the SE) and the key type must permit crypto checksum. The usage counters shall be handled as usual.

The size of DATA and RESPONSE will depend upon the algorithm reference.

10.2.5 *GET CHALLENGE Command*

Ref: As in IS 14202 for INS = '84'.

The GET CHALLENGE command will return a random number that may be derived from the session counter (but not the session counter itself). This challenge can be used implicitly only for the very next command issued by the interface device. The challenge will not be valid for the subsequent commands. The quality of the random numbers generated shall be as per prevailing international standards

10.2.6 *MANAGE SECURITY ENVIRONMENT (MSE) Command*

Ref: As in IS 14202 for INS = '22'.

The MSE command will be subjected to the following:

a) MSE SET command can only change the attributes of the current SE. Only those attributes that are listed as changeable in the table given below are permitted to be modified;

b) MSE RESTORE command can select a specified SE as the current SE. It shall operate on the SE stored in the file or as DOs in the DF; and

c) MSE STORE and MSE ERASE commands shall not be permitted.

Upon a MSE SET if the component identified by tag '94' is to be changed and it has a length 0 in the command body, then the previously obtained challenge by the GET CHALLENGE command will be used as data to derive the key. For this method to work, the MANAGE SECURITY COMMAND must be the immediately next command to execute after the GET CHALLENGE command.

The OS shall have the interpretations of the CRT as given in Table 7. The same interpretations will also be applicable for the secure messaging if applicable. In an SE (or in the argument to MSE SET) multiple tags for the changeable components might be specified. In that case, they shall be processed in the sequence of the occurrence.

When a key is derived using tag '94', its use shall be restricted only for the operations given as an argument to the MSE SET command provided the key type of the master key permits it. If the master key is not valid for the operation for which key is being derived, MSE SET command shall return an error.

Table 7 Interpretation of Various CRDOs in CRTs for an OS

(*Clause* 10.2.6)

Tag	Meaning	Applicable CRTs
Non-changeable components of an SE with MSE SET command		
'80'	Algorithm Reference (One byte value) (7.4)	AT, CT, CCT, HT
'83'	Key Reference for direct use. Use in cryptographic authentication with AT is described under INT/EXT/MUTUAL AUTH commands. For User Authentication, this tag provides the PIN identifier.	AT, CT, CCT
'84'	Key Reference for computation of session key (tags '83' and '84' to be used in mutually exclusive manner). '84' is not applicable for user auth in AT template.	AT, CT, CCT
'95'	Usage qualifier	AT, CT, CCT
Changeable components of an SE with MSE SET command (Changes are valid only for the current session and are not of permanent nature)		
'85'	(Length = 0). Set IV to zero. This may happen at the time of MSE RESTORE if this tag is used in the SE. (also the default value)	CT, CCT. For AT related commands, IV is always 0.
'86'	(Length = 0). Set the IV to zero and its update at the end of the operation, to the value of the last block (cn) of the cipher text.	CT, CCT
'87'	(Length = k) where k is the block size of the cipher for CT and CCT and value is used to set the IV.For HT (valid only for HMAC), the value is used to set the Secret Key for HMAC. (Length = 0) Increment the IV by 1 for CT and CCT.	CT, CCT, HT
'94'	Data for key derivation (valid only when '84' tag is used for key reference). Data for key derivation for 3DES/AES-128 shall be minimum 16-byte wide. Data for key derivation for AES-192shall be minimum 24-byte wide. Data for key derivation for AES-256 shall be minimum 32-byte wide.	AT, CT, CCT

10.2.7 *PERFORM SECURITY OPERATION (PSO) Command*

Ref: As in IS 14202 for INS = '2A'.

All the security operations relevant for the symmetric key cryptography will be applicable in the OS. Therefore, computation of the cryptographic checksum, calculation of a hash code, verification of the cryptographic checksum, encipherment, and decipherment will be required in the OS. These commands can be performed only if the security status satisfies the security attributes needed for the operation. Table 8 explains the P1 and P2 parameters specific to the PSO command. Further in this version, command chaining is not necessarily implemented. Hence reference to command chaining in the associated documents is not relevant.

The Encipher and Decipher operations may also implement tag '82' and '84' for the cryptogram. These tags for Encipher and Decipher operations are not mandatory in an OS. However if tag '82' is supported, the value of plaintext for the encipher operation shall be a DO as <'80' Lc DATA Padding_ if_needed>. The value returned by the decipher operation shall be only the value of tag '80' in decrypted DATA.

10.2.8 *ENABLE VERIFICATION REQUIREMENT Command*

Ref: As in IS 14202 for INS = '28'.

The enable verification requirement command will update the valid bit in EF1 for the record corresponding to the specified reference data. If P2 is given as 0, then the PIN identifier shall be taken from the current SE with the AT template for which the usage qualifier indicates the USER AUTH. The value of P1 can be 0 or 1. However, if the value of P1 is 0, the verification data present in the command body will be ignored. The command shall be executed only if the PIN repository permits update operation on the basis of current security status. Otherwise an error shall be returned.

10.2.9 *DISABLE VERIFICATION REQUIREMENT Command*

Ref: As in IS 14202 for INS = '26'.

This command will update the valid bit in EF1 for the record corresponding to the specified reference data. The value of the P2 shall be interpreted as given in Table 4. The command shall be executed only if the PIN repository permits update operation on the basis of current security status. Otherwise an error shall be returned.

10.2.10 *CHANGE REFERENCE DATA Command*

Ref: As in IS 14202 for INS = '24'.

In order to change reference data, the command may also choose an option of providing old reference data. The reference data will be updated only if one of the following conditions is satisfied (unless the reference data is invalid).

a) PIN repository permits update operation based on the current security status.
b) If the old reference data is specified in the body and its verification with the stored reference data is satisfied. The security status is also updated accordingly.
c) If the reference data is not specified in the body and the security status indicates an earlier satisfactory VERIFY command with reference to the same PIN.

The value of the P2 shall be interpreted as given in Table 4.

10.2.11 *RESET RETRY COUNTER Command*

Ref: As in IS 14202 for INS = '2C'.

The command will modify a record in the PIN repository subject to the IFD proving the knowledge of the reference data through a VERIFY command successfully completed earlier or if the PIN repository permits update operation on the basis of the current security status. If the resetting code is provided, the retry counter is set to minimum (resetting code, Max retry count). If the resetting code in not provided, the retry counter is set to the Max retry count. The resetting code will be one byte.

The value of the P2 shall be interpreted as given in Table 4.

10.3 OTHER COMMANDS

The OS shall support the commands given in **10.3.1** to **10.3.3**.

10.3.1 *GET DATA Command*

Ref: As in IS 14202 (Part 4) for INS = 'CA'.

10.3.2 *PUT DATA Command*

Ref: As in IS 14202 (Part 4) for INS = 'DA'.

10.3.3 *GET RESPONSE Command*

Ref: As in IS 14202 (Part 4) for INS = 'C0'.

11 DATA OBJECTS

In an OS, certain data objects may be made available. These shall be in compliance to the IS 14202 (Part 6). For example, some of the relevant DOs may be used to represent the Card's Sequence Number, Primary Account Number, and Cardholder's Name etc. The data objects shall be accessed using GET DATA and PUT DATA commands. DOs will be attached to a DF. GET DATA/PUT DATA commands will operate on the DOs attached to the selected DF.

The OS shall support a DO with tag '46' for pre-issuing data. This DO shall be available in the life time of the

Table 8 Interpretation of P1, P2 for PSO Commands

(*Clause* 10.2.7)

Security operation	P1 and P2 Tags	Description
Compute Cryptographic Checksum	(P1= '8E'; P2='80')	Cryptographic Checksum will be at least 4 bytes. The length of the returned value will depend upon the Le field. Also see the next row below for the description on the algorithm, IV and key references.
Verify Cryptographic Checksum	(P1 = '00'; P2= 'A2')	Data field will contain plain text (tag '80') and crypto checksum (tag '8E'). The CRT, for the operation will be known from the current SE. Algorithm reference and Key reference will be present in the SE in CCT template. The IV and IV mode update shall be as described by tags '85', '86' and '87' in the CCT template. CCT shall be subjected to the key usage DO.
Encipher	(P1 = '86'; P2 ='80')	Padding indicator byte will be '01' or '02' only.
Decipher	(P1='80'; P2 = '86')	
Hash	(P1='90'; P2='80')	Algorithm reference will be taken from HT template. If not present, '00' (default) shall be taken as algorithm reference.

ICC and shall be used to return the chip serial number of the chip embedded in the ICC and as provided by the chip manufacturer. The embedded chips for the OS must support the way of providing a unique chip serial number which will be returned by GET DATA command. PUT DATA command for DO '46' will not modify the value and return an appropriate error. The DO '46' shall be available at least in the MF and shall have variable length.

SECTION II : CRYPTOGRAPHIC INFRASTRUCTURE IN SCOSTA

12 SECURE MESSAGING (SM)

The SM for OS shall be indicated by tCLA byte being '08' or '0C' in the tAPDU. The SM may incorporate confidentiality, integrity, both or none. When an SM does not incorporate the integrity, the only possible value for the tCLA shall be '08' and the command header will not be authenticated.

The following fields of the APDU shall be subjected to the SM while computing tAPDU.

a) Command Header (including CLA, INS, P1 and P2),
b) Command Data Field (DATA),
c) Le field,
d) Response Data Field (RESPONSE), and
e) Response Status Bytes (SW1, SW2).

Under the SM, the command data field in the tAPDU(tDATA) shall be consisting of collection of the SM related DOs which can include the fields given in Table 9.

Table 9 SM Fields for Secure Messaging

(*Clause* 12)

SM Tags	Meaning of Value	Explanatory Notes
'80', '81'	DATA field of APDU in case of command and RESPONSE field of APDU in case of response.	
'82', '83'	Data fields provide a cryptogram. After decryption of the cryptogram, the plaintext provides the SM_Dos with tags as listed in this table (and will not include DOs with tags '82', '83', 'B0' and 'B1').	There shall be only a maximum of one field each of the DATA, Le, command header in the command APDU and only a maximum of one field each of the RESPONSE and SW1-SW2 in the response APDU. Thus a tag '80' or '81' may be found in the plaintext corresponding to tag '82' or as a DO in the tDATA field. The value field of this DO is a context by itself and may include crypto-checksum (tag '8E'). The key and algorithm shall be from the CT template in the SM field or from the current SE (if not specified in the SM field).
'86', '87'	Padded if necessary and encrypted DATA field of the command APDU and RESPONSE field of the response APDU.	The Lc field and Le field shall be known after decryption and removal of padding as length of the data. The key and algorithms shall be taken as described in the explanting notes for SM tags '82'/'83'.
'89'	Command Header of the APDU (CLA-INS-P1-P2)	Command Header may be given in the tAPDU data field. In that case, the Command Header of the tAPDU (tCLA-tINS-tP1-tP2) shall be ignored for the command execution. tCLA shall be used to formulate the response APDU only. If this tag is used, the use of integrity mechanism is mandatory.
'8E'	Crypto-Checksum	When used, this shall be the last field in the context. If used in under the plaintext corresponding to SM-DOs with tags '82' and '83' or value field in corresponding to tags SM-DOs 'B0' and 'B1', '8E' shall be the last DO. When used in the context of the tDATA or tRESPONSE, it shall be the last field of the tDATA or tRESPONSE. The crypto-checksum shall be computed/verified using the CCT template ('B4'/'B5') provided in the SM field in the same context, or the CCT template of the current SE.
'96', '97'	Provides the value of the Le.	This SM field is valid only in the command tAPDU.
'99'	Provides the SW1 and SW2	This SM field is valid only in the response tAPDU.
'B0', 'B1'	Plaintext DOs whose values include the SM fields as described in this table and shall not include SMDos with tags '82', '83', 'B0' or B1'.	The value field is a context by itself and may include cryptochecksum (tag '8E') of relevant DOs in the value.
'B4', 'B5'	CCT template	In the context where this DO is found, the crypto-checksum is computed using the values of this DO.
'B8', 'B9'	CT template	In the context where this DO is found, the encryption/decryption is carried out using the values of this DO.

The following shall be applicable for the secure messaging:

a) If the CCT and/or CT templates are not provided in the SM data fields, then the CCT and/or CT templates of the current SE shall be used.

b) The DATA and RESPONSE fields may be found in one of the following places:
   1) As a plaintext value with tags '80'/'81';
   2) As the decrypted and de-padded cipher text from tags '86'/'87';
   3) While processing the DOs for the value fields of plaintext DOs 'B0'/'B1'; and
   4) While processing the DOs for the values fields of the decrypted and de-padded cipher-text from tags '82'/'83'.

c) The Le and SW1/SW2 fields may be found in one of the following places:
   1) As value in DOs with tags '96'/'97' for Le and '99' for SW1-SW2.

d) Under tags '82'/'83' whose value field when decrypted and de-padded provides collection of DOs which may include DOs with tags '96'/'97' for the Le and '99' for SW1-SW2.

e) The tDATA field and tRESPONSE fields of the tAPDU may include several contexts. Each context provides a collection of SM DOs. A new context starts in SM DOs with tags '82'/'83'/'B0'/'B1'. Each context may include zero or one CCT template, zero or one CT template and zero or one crypto-checksum. The crypto checksum if present shall be the last DO in its context.

f) When the CCT and CT templates are usedin the SM fields, these may refer to the derived keys.

g) In a context, the crypto-checksum shall be computed for all DOs which have an odd tag. The computation of the checksum shall be subjected to the padding as defined in ISO/IEC 7816-4 and to the crypto-checksum algorithms as described in this standard.

h) Each time an encryption/decryption is performed, the key usage counters shall be updated as defined for the PSO command.

j) Keys and Algorithms used for formulating the tRESPONSE will be determined on the basis of following in the given order:
   1) The CRTs given in the command APDU which are applicable for SM response and
   2) The CRTs in the current SE applicable for SM response.

13 SESSION KEY DERIVATION

The OS shall maintain at least two session keys, one for the confidentiality and another for the integrity. In case the derived keys are to be used for the authentication purposes as well, these may share space with the session keys for the confidentiality (that is, there may be only one derived key for authentication and confidentiality). When the keys are derived, the OS shall have to maintain the usage for which the key is derived and permit only that use.

The OS shall be able to derive the session keys using one of the methods given in **13.1** to **13.3**.

13.1 Authentication along with Session Key Derivation

Session key can be derived along with the authentication using GET CHALLENGE and MUTUAL AUTHENTICATE command. This has been described in **15.3** when the algorithm reference is 2. Two keys shall be derived in this manner, one for the confidentiality and another for the integrity. The confidentiality key shall be usable for encryption and decryption (this can be restricted further by the CRT usage tag '95' in the CT template in the current SE). The integrity key shall be usable for the computation and verification of cryptographic checksum (this can be restricted further by the CRT usage tag '95' in the CCT template).

13.2 Session Key Derivation using MANAGE SECURITY ENVIRONMENT Command

The MANAGE SECURITY ENVIRONMENT can be used for the key derivation of the session keys. For this tag '94' in the appropriate CRT shall be used. For example, if the CT template of the current SE is selected, the key shall be derived for the confidentiality as per the key usage qualifier in that SE. The key derivation method shall use the tag '84' (in theappropriate CRT) to find the key reference of the master key. It shall also check if the key is permitted as a master key in the key repository. The key derivation shall use algorithm reference for the algorithm for generation.

Based on algorithm used for key derivation, the derived key shall be taken as higher order bytes of length equal to the size of the key from the cryptogram generated by encryption of data under '94' tag using the corresponding encryption algorithm. The padding on the data (plain text) under '94' tag shall be '80' followed by zero or more bytes of all zeroes if applicable.

The IV shall be taken as 0 (and it shall not modify the IV for confidentiality/integrity maintained separately by the OS). The encryption mode will be CBC. The resulting key shall be subjected to the key usage based on the key type parameter in the key repository. Thus a key derived using the CT template for example, can be made to work only for encryption or only for decryption or for both.

13.3 Key Derivation for Authentication

Keys may be derived for the authentication purposes if the corresponding master key reference is provided

in the AT template in the current SE. The algorithm for the key derivation is the same as that for the session key derivation using MANAGE SECURITY ENVIRONMENT command as described in **13.2**.

14 SETTING INITIAL VALUE (IV) FOR CRYPTOGRAPHIC METHODS

Many cryptographic algorithms require an initial value (IV), size of which usually depends upon the algorithm. Each cryptographic operation may in turn update the IV at the end. There are the following possibilities for the IV value and IV update: The value of the IV is set as per the details given in Table 7. IV is also updated at the end of the cryptographic operation as given in Table 7.

Initial value of the IV may also be determined as defined in **15.3** for authentication and session key establishment.

The OS shall maintain two different IVs and IV update modes, one each for the confidentiality and integrity. IV for integrity shall be updated at the end of computation/verification of cryptographic checksum and IV for confidentiality shall be updated at the end of encryption/decryption by means of a PSO command or by means of a secure messaging.

15 CRYPTOGRAPHIC ALGORITHMS

The OS shall support all cryptographic algorithms as described in **7.4** (Table 1). In this section, the algorithms are described in details.

15.1 Algorithms for Confidentiality

Algorithms for the confidentiality include algorithms for Encryption and Decryption. The OS shall support 3DES along with AES-128/192/256 algorithm. These algorithms shall be subjected to padding (as defined in ISO 9797-1 padding method 2) as well as CBC mode of encryption/decryption. The algorithm reference of '00' and '01' in the CT template in a CRT shall mean the 3DES algorithm. The algorithm reference of '82', '83' and '84'in the CT template in a CRT shall mean the algorithms AES-128, AES-192 and AES-256 respectively.

The IV for the algorithms and the method to update the IV at the end of encryption/decryption can be set by MANAGE SECURITY ENVIRONMENT command.

Only one IV need be maintained by the OS for the confidentiality which shall be different from the IV maintained by the OS for the integrity.

The 3DES algorithm is explained pictorially in Fig. 1 and Fig. 2. The implementation in Fig. 2 shall be applicable to AES algorithms as well with 3DES blocks replaced by AES-128 or AES-192 or AES-256 blocks.

Depending upon the value of the IV related tags, the new value of the IV may be set automatically to cn (the last cipher-text block) when the chaining mode is used for the IV.

The IV must be initialized whenever the current SE is changed (for example, because of SELECT FILE command or by MANAGE SECURITY ENVIRONMENT command).

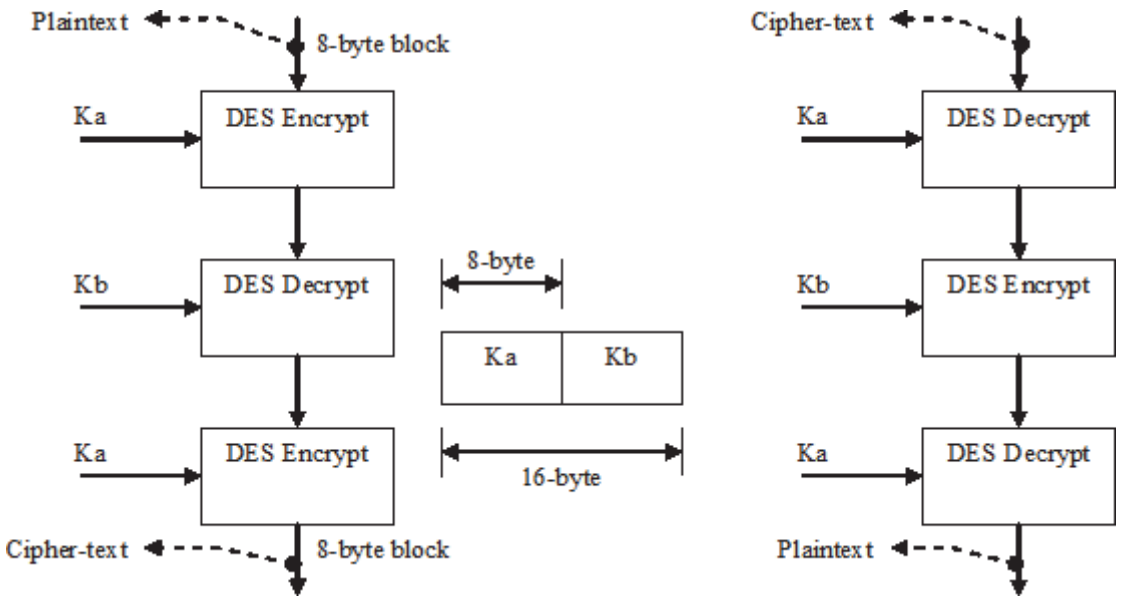


FIG. 1 BASIC ENCRYPTION AND DECRYPTION MECHANISMS IN 3 DES ALGORITHM

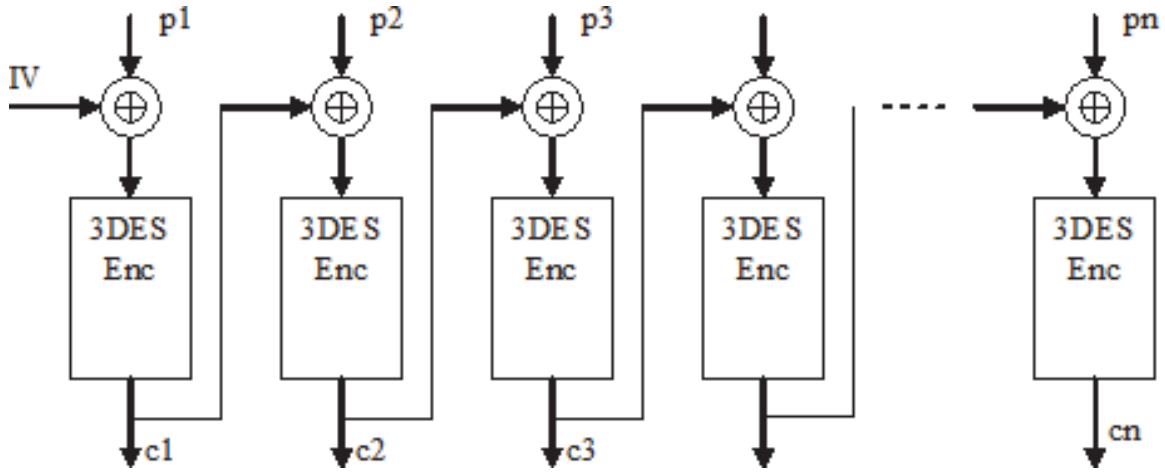


FIG. 2 3 DES ENCRYPTION OF LARGE MESSAGES USING CBC MODE

15.2 Algorithms for Integrity

The OS shall support five algorithms for the integrity. The first algorithm (known as 3DES based CBC residue) is ISO/IEC 9797-1 MAC algorithm 1 and shall be indicated by algorithm reference of '01' in the CCT template of the CRT. The second algorithm is ISO/IEC 9797-1 algorithm 2 for MAC using DES shall be indicated by algorithm reference of '00' or '02'. The third through fifth algorithms are ISO/IEC 9797-1 algorithm 1 for MAC using AES-128, AES-192 and AES-256 respectively and shall be indicated by algorithm references of '83', '84' or '85'. The algorithms may need an IV which shall be taken as IV for the integrity template.

15.2.1 *CBC Residue based Integrity (ISO/IEC 9797-1 MAC algorithm 1)*

In this mode, the 3DES algorithm shall be used for large messages. The integrity code (or cryptographic checksum) shall be derived from the cn (the last block of the encryption as shown in Fig. 2). It is recommended that an application should not use identical keys for confidentiality and integrity.

The cryptographic checksum (or the integrity code) shall be at least 4 bytes long and at most 8 bytes long (the size of the cn in 3DES). In case, smaller than 8 bytes are used for the integrity code, those many bytes from the least significant bytes onward shall be returned out of the CBC residue. The IV and the method to update IV shall be governed by the appropriate tags in the CCT template of the CRT. The operations will be similar to the ones described earlier.

15.2.2 *ISO/IEC 9797-1 MAC Algorithm 2*

This algorithm shall be indicated by the algorithm reference of 2 in the CCT template of the CRT to an OS. In this mode, IV shall be first incremented by 1 and shall not be updated at the end of the computations. This algorithm is represented in Fig. 3.

15.2.3 *CBC Residue based Integrity Using AES-128 (ISO/IEC 9797-1 MAC algorithm 1)*

This algorithm (known as CBC residue based integrity using AES-128) is ISO/IEC 9797-1 MAC algorithm 1 with AES-128 and shall be indicated by algorithm reference of '83' in the CCT template of CRT. The cryptographic checksum (or the integrity code) shall be atleast 8 bytes long and maximum 16 bytes long (the size of the cn in Fig 2 with 3DES replaced by AES-128). In case, less than 16 bytes are used for the integrity code, those many bytes from the least significant bytes onward shall be used out of the CBC residue. The IV and the method to update IV shall be governed by the appropriate tags in the CCT template of the CRT. The operations will be similar to the ones described earlier.

15.2.4 *CBC Residue based Integrity Using AES-192 (ISO/IEC 9797-1 MAC algorithm 1)*

This algorithm (known as CBC Residue based integrity using AES-192) is ISO/IEC 9797-1 MAC algorithm 1 with AES-192 and shall be indicated by algorithm reference of '84' in the CCT template of CRT. Other details shall be same as for AES-128 based residue.

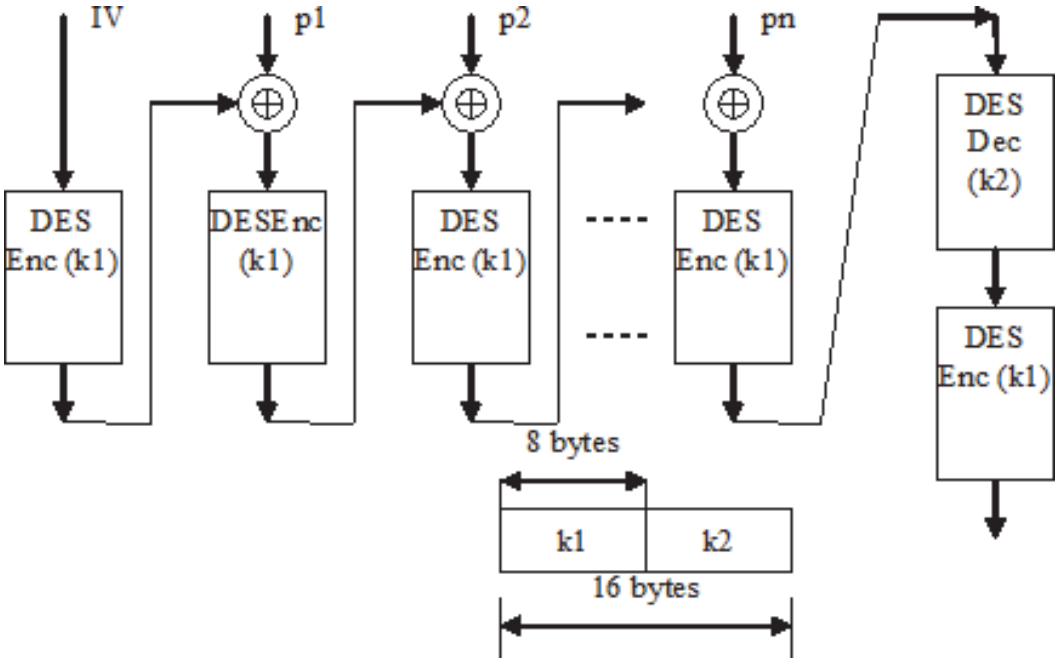


FIG. 3 ISO/IEC 9797-1 MAC ALGORITHM 2 USING DES

15.2.5 *CBC Residue based Integrity Using AES-256 (ISO/IEC 9797-1 MAC algorithm 1)*

This algorithm (known as CBC Residue based integrity using AES-256) is ISO/IEC 9797-1 MAC algorithm 1 with AES-256 and shall be indicated by algorithm reference of '85' in the CCT template of CRT. Other details shall be same as for AES-128 based residue.

15.3 Algorithms for Authentication

There shall be at least five algorithms for cryptographic authentication (INTERNAL, EXTERNAL and MUTUAL AUTH).

The algorithm reference of '00' or '01' shall refer to the 3DES based challenge response method. In this method, a challenge of 8 bytes shall be given by the challenger (IFD or ICC) to the subject (ICC or IFD). The subject shall encrypt the challenge using the indicated key and provide 8-byte response obtained as cipher-text from the 3DES encryption as described in Fig. 1.

The algorithm reference of '02' shall refer to the 3DES based authentication as well as session key establishment of ISO/IEC 11770-2 key establishment mechanism and as described in Fig. 4.

The algorithm reference of '83' shall refer to AES-128 based challenge response method. In this method, a challenge of 16 bytes shall be given by the challenger (IFD or ICC) to the subject (ICC or IFD). The subject shall encrypt the challenge using the indicated key and provide 16-byte response obtained as cipher-text from AES-128 encryption.

The algorithm reference of '84' shall refer to AES-192 based challenge response method. In this method, a challenge of 16 bytes shall be given by the challenger (IFD or ICC) to the subject (ICC or IFD). The subject shall encrypt the challenge using the indicated key and provide 16-byte response obtained as cipher-text from AES-192 encryption.

The algorithm reference of '85' shall refer to AES-256 based challenge response method. In this method, a challenge of 16 bytes shall be given by the challenger (IFD or ICC) to the subject (ICC or IFD). The subject shall encrypt the challenge using the indicated key and provide 16-byte response obtained as cipher-text from AES-256 encryption.

15.4 Algorithm for Hash

The OS shall use the SHA-1 algorithm as described in FIPS-140 (ISO/IEC 19790) for message digest operations when algorithm reference '00' and '01' are used in the HT template. OS shall use SHA-256 algorithm when algorithm reference '02' is used in the HT template. OS shall use HMAC algorithm with SHA1 when algorithm reference is '03'. OS shall use HMAC algorithm with SHA-256 when algorithm reference is '04'. The maximum size of the data to be hashed shall not exceed more than 255 bytes.

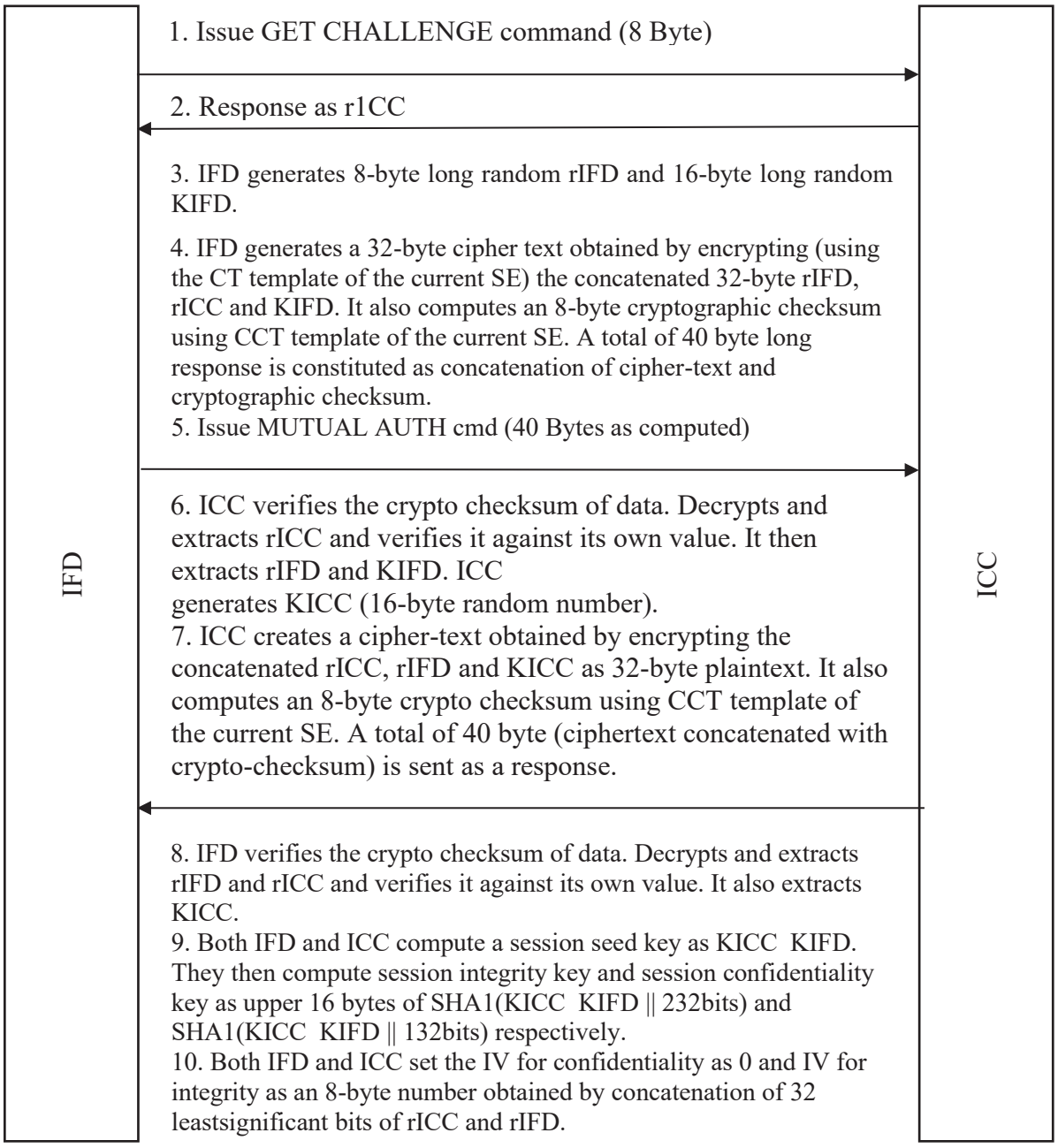

IFD
ICC
1. Issue GET CHALLENGE command (8 Byte)
2. Response as r1CC
3. IFD generates 8-byte long random rIFD and 16-byte long random KIFD.
4. IFD generates a 32-byte cipher text obtained by encrypting (using the CT template of the current SE) the concatenated 32-byte rIFD, rICC and KIFD. It also computes an 8-byte cryptographic checksum using CCT template of the current SE. A total of 40 byte long response is constituted as concatenation of cipher-text and cryptographic checksum.
5. Issue MUTUAL AUTH cmd (40 Bytes as computed)
6. ICC verifies the crypto checksum of data. Decrypts and extracts rICC and verifies it against its own value. It then extracts rIFD and KIFD. ICC generates KICC (16-byte random number).
7. ICC creates a cipher-text obtained by encrypting the concatenated rICC, rIFD and KICC as 32-byte plaintext. It also computes an 8-byte crypto checksum using CCT template of the current SE. A total of 40 byte (ciphertext concatenated with crypto-checksum) is sent as a response.
8. IFD verifies the crypto checksum of data. Decrypts and extracts rIFD and rICC and verifies it against its own value. It also extracts KICC.
9. Both IFD and ICC compute a session seed key as KICC KIFD. They then compute session integrity key and session confidentiality key as upper 16 bytes of SHA1(KICC KIFD || 232bits) and SHA1(KICC KIFD || 132bits) respectively.
10. Both IFD and ICC set the IV for confidentiality as 0 and IV for integrity as an 8-byte number obtained by concatenation of 32 leastsignificant bits of rICC and rIFD.

FIG. 4 AUTHENTICATION AND KEY ESTABLISHMENT PROTOCOL

ANNEX A

(*Clause* 2)

REFERENCES

A-1 LIST OF REFERRED INDIAN STANDARDS

IS No.	*Title*
14202 (Part 1) : 2014/ ISO/IEC 7816-1 : 2011	Identification cards — Integrated circuit cards: Part 1 cards with contacts — Physical characteristics (*second revision*)
14202 (Part 2) : 2014/ ISO/IEC 7816-2 : 2007	Identification cards — Integrated circuit cards: Part 2 cards with contacts — Dimensions and location of the contacts (*second revision*)
14202 (Part 3) : 2013/ ISO/IEC 7816-3 : 2006	Identification cards — Integrated circuit cards: Part 3 Cards with contacts — Electrical interface and transmission protocols (*first revision*)
14202 (Part 4) : 2021/ ISO/IEC7816-4 : 2020	Identification cards — Integrated circuit cards: Part 4 Organization: Security and commands for interchange
14202 (Part 6) : 2018/ ISO/IEC 7816-6 : 2016	Identification cards — Integrated circuit cards: Part 6 Interindustry data elements for interchange (*second revision*)
14202 (Part 8) : 2013/ ISO/IEC 7816-8 : 2004	Identification cards — Integrated circuit cards: Part 8 Commands for security operations
14202 (Part 9) : 2013/ ISO/IEC 7816-9 : 2004	Identification cards — Integrated circuit cards: Part 9 Commands for card management
14202 (Part 15) : 2021/ ISO/IEC 7816-15 : 2016	Identification cards — Integrated circuit cards: Part 15 Cryptographic information application
IS/ISO/IEC 11770-2 : 2018	IT security techniques — Key management: Part 2 Mechanisms using symmetric techniques (*first revision*)

A-2 LIST OF REFERRED INTERNATIONAL STANDARDS / PUBLICATIONS

ISO/IEC No.	*Title*
ISO/IEC 14443-3 : 2011	Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anti-collision
ISO/IEC 14443-4 : 2008	Identification cards — 2008 Contactless integrated circuit cards — Proximity cards: Part 4 Transmission protocol
ISO/IEC 7501-1 : 2008	Identification cards — Machine 2008 readable travel documents — Part 1: Machine readable passport
ISO/IEC 9797-1	Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
ISO/IEC 19790	Information technology — Security techniques — Security requirements for cryptographic modules

ANNEX B

(*Foreword*)

COMMITTEE COMPOSITION

Computer Hardware, Peripherals & Identification Cards Sectional Committee, LITD 16

Organization	*Representative(s)*
In personal capacity	Dr Mahesh Chandra (***Chairman***)
All India Radio, New Delhi	Mr S. K. Srivastava Mr Pradeep Mehra (*Alternate*)
Canon India Private Limited, Gurugram	Mr Ashish Khaana Mr Satoshi Hirabayashi (*Alternate*)
Central Institute of Plastics Engineering and Technology, Murthal	Dr Smita Mohanty Dr M. R. Biswal (*Alternate*)
Centre for Development of Advanced Computing, Noida	Ms Savita Kashyap Mr Rajesh Kushwaha (*Alternate*)
Centre for Railway Information Systems, New Delhi	Mr G. K. Maishi Mr Vijay K. Devnath (*Alternate*)
Computer Society of India, New Delhi	Prof M. N. Hoda
Delhi Integrated Multi-Modal Transit System Ltd, New Delhi	Mr Alok Sethi Mr Abhishek Srivastava (*Alternate*)
Delhi Metro Rail Corporation Limited, Delhi	Mr V. P. Singh
Electronics Regional and Test Laboratory (North), New Delhi	Mr M. P. Sharma
e-Smart Systems Limited, New Delhi	Mr Anurag Ashok
Fime India, Bengaluru	Mr Hardik Mirani Mr Angaj Bhandari (*Alternate*)
HP India Sales Private Limited, Bengaluru	Ms Anubhuti Ms Upasana Choudhry (*Alternate*)
In personal capacity	Mr Vinay Bhushan Taneja
Indian Institute of Technology Bhilai, Bhilai	Prof Rajat Moona
Infineon Technologies India Private Limited, Noida	Mr Madhusudhanan Sampath Mr Ajay Hanyalu (*Alternate*)
Manufacturers Association for Information Technology, New Delhi	Mr George Paul
Ministry of Electronics and Information Technology-Standardization Testing and Quality Certification (STQC), New Delhi	Mr Manish Selal
Ministry of Electronics and Information Technology, New Delhi	Mr Mukul Kumar Yadav Mr U. K. Nandwani (*Alternate* I) Shrimati Asha Nangia (*Alternate* II)
Narnix Technolabs Private Limited, New Delhi	Mr N. Kishor Narang
National Informatics Centre, New Delhi	Mr Rajdeep Choudhury
National Payments Corporation of India, Mumbai	Mr Nalin Bansal Mr Sanjay Chandak (*Alternate*)
NXP Semiconductors India Private Limited, Bengaluru	Mr Ajesh Kapoor Mr Achin Jain (*Alternate*)

Organization	*Representative(s)*
Samsung India Electronics Private Limited, New Delhi	Mr Deepak Bharadwaj Mr Sanjay Kumar Bansal (*Alternate*)
ST Microelectronics Private Limited, Greater Noida	Mr Prashant Pandey
Telecommunication Engineering Center, New Delhi	Mr R. Saji Kumar Mr Uttam Chand (*Alternate*)
The Institution of Electronics and Telecommunication Engineers, New Delhi	Prof WG CD P. Prabhakar Dr Jyotsna Kumar Mandal (*Alternate*)
UL India Private Limited, Bengaluru	Mr Ashish Mathur Mr V. Manjunath (*Alternate*)
BIS Director General	Ms Reena Garg, Scientist 'F' and Head (Electronics and IT) [Representing Director General (*Ex-officio*)]

Member Secretary

Shri Manikandan K.
Scientist 'D' (Electronics and IT), BIS

Panel involved in the Finalization – LITD 16 : 1 Cards and personal Identification

Organization	*Representative(s)*
Indian Institute of Technology Bhilai, Bhilai	Prof Rajat Moona (***Convener***)
Centre for Development of Advanced Computing, NOIDA	Ms Savita Kashyap
Centre for Development of Advanced Computing, NOIDA	Mr Adarsh Pillai
Centre for Development of Advanced Computing, NOIDA	Mr Manish Kumar Verma
e-Smart Systems Limited, New Delhi	Mr Anurag Ashok
Infineon Technologies India Private Limited, Noida	Mr Madhusudhanan Sampath
Manufacturers Association for Information Technology, New Delhi	Mr George Paul
NXP Semiconductors India Private Limited, Bengaluru	Mr Ajesh Kapoor
National Informatics Centre, New Delhi	Mr Rajdeep Choudhury
ST Microelectronics Private Limited, Greater Noida	Mr Deepak Agarwal
ST Microelectronics Private Limited, Greater Noida	Mr Prashant Pandey

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 16 (16518).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg, NEW DELHI 110002	2323 7617, 2323 3841
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi, KOLKATA 700054	2337 8499, 2337 8561, 2337 8626, 2337 9120
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg, CHANDIGARH 160019	265 0206, 265 0290
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442, 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East), MUMBAI 400093	2832 9295, 2832 7858, 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi